IN THE UNITED STATES DISTRICT COURT
FOR THE NORTHERN DISTRICT OF GEORGIA
ATLANTA DIVISION

In re: Equifax, Inc. Customer Data Security Breach Litigation	)	MDL Docket No. 2800
	)	Case No.: 1:17-md-2800-TWT
	)	**CONSUMER ACTIONS**

CONSUMER PLAINTIFFS' MEMORANDUM OF LAW IN OPPOSITION TO EQUIFAX'S MOTION TO DISMISS THE COMPLAINT

TABLE OF CONTENTS

TABLE OF CASES

"We at Equifax clearly understood that the collection of American consumer information and data carries with it enormous responsibility to protect that data. We did not live up to that responsibility."

Richard F. Smith, Equifax's former Chief Executive Officer

INTRODUCTION

As one of the world's largest custodians of consumer data, Equifax publicly refers to itself as a "trusted steward" of consumer data and declares that the security of consumer information is "paramount." In this litigation, however, while continuing to profess its commitment to data security, Equifax contends it has *no legal duty* to secure the highly sensitive information it collects and should face *no legal liability whatsoever* for the most notorious data breach in our nation's history, a breach that has already caused economic loss to millions of consumers and subjected nearly 150 million Americans to a substantial and imminent risk of identity theft and fraud that will continue so long as Social Security numbers play a role in their financial lives. Equifax also contends that whether its existing data security measures are adequate to prevent another breach and avoid causing even more harm to consumers is an issue beyond the reach of this or any Court.

To justify these contentions, Equifax marginalizes—or simply ignores—this Court's decisions recognizing a legal duty and potential liability for its breach in similar circumstances. *See, e.g.*, *In re Arby's Rest. Grp. Inc. Litig*., ("*Arby's*"),

2018 WL 2128441, at *5 (N.D. Ga. Mar. 5, 2018) ("[A]llegations that a company knew of a foreseeable risk to its data security systems are sufficient to establish the existence of a plausible legal duty to survive a motion to dismiss."); *In re The Home Depot, Inc., Customer Data Security Breach Litig*., ("*Home Depot*"), 2016 WL 2897520, at *3 (N.D. Ga. May 18, 2016) ("A retailer's actions and inactions, such as disabling security features and ignoring warning signs of a data breach, are sufficient to show that the retailer caused foreseeable harm to a plaintiff and therefore owed a duty in tort."). Because the *McConnell* opinions that serve as the cornerstone of Equifax's motion do not address foreseeability, they are inapposite.

Equifax likewise ignores *Home Depot* and *Arby's*, and a wealth of precedent from across the country, on various other points:

- Equifax does not challenge Article III standing, but argues Plaintiffs have not suffered any legally recognizable harm notwithstanding allegations that class members spent time and money addressing identity theft and fraud, purchased credit monitoring and credit freezes to mitigate possible harm as suggested by Equifax, and had unauthorized withdrawals from their accounts, all of which in fact are legally sufficient injuries;

- The economic loss doctrine does not bar negligence claims where there is an "independent duty of care" imposed by law;

- Proximate cause is adequately pleaded and is uniquely a jury question;

- Deficient cybersecurity constitutes an "unfair practice" for purposes of a claim for negligence per se predicated on the Federal Trade Commission Act and asserting a claim under the Georgia Fair Business Practices Act;

- Plaintiffs' Fair Credit Reporting Act claims, challenging the most egregious failure of cybersecurity by a credit reporting agency, further the intent of Congress to address concerns about abuses in the industry and promote the underlying statutory purpose to protect consumer privacy;

- Equifax's misrepresentations and omissions and shoddy data security are actionable under state consumer protection statutes.

The Court should reject Equifax's self-serving claims of immunity and deny the pending motion in its entirety.

BACKGROUND

Equifax is one of three major credit reporting agencies ("CRA") that control the market for consumer credit information. Compl. ¶¶ 122-27, 133. Equifax's business model involves aggregating consumer data in credit reports and selling those reports to other businesses. *Id.* ¶ 134. Equifax recognizes its value as a company is inextricably tied to its massive trove of consumer data and, as a result, has implemented a simple strategy: "Gather as much personal data as possible and find new ways to sell it." *Id.* ¶ 145, 137. Equifax now maintains information on over 820 million individuals worldwide. *Id.* ¶¶ 133-44.

Before the 2017 breach, Equifax understood the repercussions of failing to secure confidential consumer information, knew it was a potential target for hackers, and was on explicit notice that its data security was inadequate. The company even held itself out as expert in anticipating and combatting cybersecurity threats and sold "data breach solutions" intended to combat the "great risk of identity theft and fraud." *Id.* ¶ 147. Equifax observed major data breaches at other corporations such as Target, Home Depot, Anthem, and its competitor Experian. *Id.* ¶¶ 159-65. Indeed, Equifax *itself* was subject to several breaches. *Id*. ¶¶ 166-82. And, experts warned Equifax about its critical data security problems; one even predicted that the risk of an imminent breach at Equifax was 50 percent. *Id.* ¶ 179.

Nonetheless, Equifax did little, if anything, to strengthen its cybersecurity defenses, which were woefully deficient as a result of systemic incompetence and the lackluster approach to data security permeating the company's culture. *See, e.g.*, *id.* ¶¶ 216-19. Equifax viewed the threat posed by hackers as simply another business opportunity from which it could profit. While short changing its own data security, Equifax spent millions acquiring two companies—Trusted ID and ID Watchdog—so that it could sell more identity theft protection services to

consumers, *id.* ¶ 146, which Equifax's CEO touted as a "huge opportunity" and "massive, growing business." *Id.* ¶ 165.

Given Equifax's longstanding, cavalier attitude toward data security, a massive breach was all but inevitable and, in fact, one occurred in 2017 due to an inexcusable series of missteps. On March 6, 2017, a serious vulnerability was discovered in Apache Struts, a free, open-source program used by Equifax to power its consumer dispute website. *Id.* ¶¶ 183-86. The next day, the Apache Software Foundation issued a free "patch" and urged all users to immediately install it. *Id*. ¶ 187. On March 8, the Department of Homeland Security issued its own warning, reflecting the seriousness of the risk. *Id*. ¶ 188. Equifax disseminated the warning internally, but never installed the patch, even though it ran scans that should have caught the problem. *Id*. ¶¶ 189, 192. Beginning on May 13, 2017, two months after the patch became available, hackers exploited the Apache Struts vulnerability to access Equifax's computer network, remained undetected until July 30, 2017 because the company lacked systems to discover their presence, *id*. ¶ 194, and exfiltrated the personal information of nearly 150 million Americans. *Id*. ¶ 195.

Equifax waited more than five weeks to publicly announce the breach, depriving consumers of the chance to take immediate precautions. *Id*. ¶ 227. When

the announcement was finally made, Equifax acknowledged that hackers had obtained "names, Social Security numbers, birth dates, addresses and, in some instances, driver's license numbers" of at least 143 million Americans. *Id*. ¶ 228. Equifax later revealed that millions more had been affected and the stolen data included gender, phone numbers, tax ID numbers, driver's license information, email addresses, and payment card information. *See id*. ¶ 212.

The impact of the breach is severe. As one analyst noted soon after the breach was announced: "On a scale of 1 to 10 in terms of risk to consumers, this is a 10." *Id.* ¶ 4. Equifax acknowledged the risk and advised consumers to take precautions by visiting a website to see whether they were affected and purchasing "credit freezes" to prevent fraud. At Equifax's urging, millions of consumers paid to freeze their credit. *Id*. ¶¶ 263-65. While Equifax agreed to waive its fees for a limited period of time, consumers had to pay to freeze their credit at Experian and TransUnion. *Id*. ¶ 264. In addition to fees incurred freezing their credit, consumers have had to spend time and money taking other steps to protect themselves from the misuse of their data and many have had to deal with instances of identity theft, unauthorized credit card use, fraudulent accounts, and similar problems as a direct result of the breach. *Id*. ¶ 294.

The stories of the five Georgia class representatives exemplify the harm suffered by the other class members:

- John Simmons II suffered identity theft and had unauthorized accounts opened in his name. He had to file a police report, place a fraud alert on his credit file, deal with creditors on the fraudulent accounts, and his home loan was delayed because his credit score dropped. *Id.* ¶ 37.

- Wanda Paulo spent time and money freezing her credit. *Id.* ¶ 34.

- Justin O'Dell spent time monitoring his financial accounts for fraud and bought credit monitoring services. *Id.* ¶ 35.

- Michael Chase paid for credit freezes and credit monitoring and spent time and effort trying to get timely and accurate information out of Equifax. *Id.* ¶ 36.

- Sylvia Patterson's identity was stolen as a result of the breach, forcing her to file reports with the police and IRS, freeze her credit, and buy credit monitoring services. *Id.* ¶ 38.

Moreover, these Georgians, along with all other class members, remain at a substantial and imminent risk of future harm because of Equifax's deficient cybersecurity measures. *See, e.g., id.* ¶¶ 34-38, 282-95.

While purporting to accept the truth of these allegations, Equifax's brief is replete with unsupported "alternative facts" attempting to create the illusion of a universe in which the breach never occurred and, even if it did, no one was harmed. For example, Equifax claims that its businesses "built a strong security

infrastructure to protect the information they receive, maintain, and send," Mot. 1—a claim belied by the breach itself; Plaintiffs' allegations of the company's shoddy data security practices; the admissions of its CEO; and analyses of independent experts, including the damning report issued by Senator Elizabeth Warren in February 2018 concluding the breach occurred because "Equifax adopted weak cybersecurity measures that failed to protect consumer data – a symptom of what appeared to be the low priority afforded cybersecurity by company leaders." Compl. ¶¶ 215-16. Similarly, Equifax claims "it is not likely that any Plaintiff will suffer future harm," despite Plaintiffs' specific allegations to the contrary and the company's own advice to consumers of the need to take precautions. *See* Mot. 18 (compare with Compl. ¶¶ 11-108; 282-95). But this Court must decide the motion to dismiss in this universe, based on Plaintiffs' allegations, and not on alternative facts. Plaintiffs' claims are factually plausible and legally sufficient. The motion should be denied.

LEGAL STANDARD & CHOICE OF LAW

A complaint may only be dismissed if the facts alleged fail to state a "plausible" claim. *Home Depot*, 2016 WL 2897520, at *3 (citing *Ashcroft v. Iqbal*, 556 U.S. 662, 677 (2009); Fed. R. Civ. P. 12(b)(6)). A claim survives even if it is "improbable" a plaintiff will be able to prove those facts or the odds of recovery

are "remote and unlikely." *Id.* (citing *Bell Atlantic v. Twombly*, 550 U.S. 544, 556 (2007)). "[T]he court must accept the facts pleaded in the complaint as true and construe them in the light most favorable to the plaintiff." *Id.*

Equifax asserts that Georgia law applies to the common law claims for purposes of this motion. Mot. 11. Plaintiffs agree that the Court need not apply the common law of other states, unless it decides that Georgia law is adverse to the common law claims of the national class pled in the Complaint, in which case it will be necessary to consider the common law of each state applicable to the proposed alternative, state-specific classes. *See* Compl. ¶ 297 (pleading alternative claims based on the common law of each state).

ARGUMENT

I. PLAINTIFFS' NATIONWIDE CLAIMS SHOULD PROCEED.

A. Plaintiffs Adequately Plead A Negligence Claim.

1. The Complaint Alleges A Recognized Legal Duty.

Under Georgia law, "allegations that a company knew of a foreseeable risk to its data security systems are sufficient to establish the existence of a plausible legal duty and survive a motion to dismiss." *Arby's*, 2018 WL 2128441, at *5. Put another way: "A retailer's actions and inactions, such as disabling security features and ignoring warning signs of a data breach, are sufficient to show that the retailer caused foreseeable harm to a plaintiff and therefore owed a duty in tort." *Home*

Depot, 2016 WL 2897520, at *3; *see also In re Target Corp. Data Sec. Breach Litig.*, 66 F. Supp. 3d 1154, 1173 (D. Minn. 2014) (applying Georgia law).[1]

Such allegations are the bedrock of the Complaint: Despite Equifax's critical role in the consumer credit system and appreciation of the risk of a massive data breach, Equifax had objectively deficient security measures; ignored repeated red flags and warnings that drastic improvements were needed; neglected to install a software patch that it knew was critical; and never bothered to implement basic security measures to detect and monitor unauthorized activity on its network. *See generally* Compl. ¶¶ 187-95, 227-90. As in *Home Depot* and *Arby's*, these detailed allegations show that Equifax owed Plaintiffs a duty not to subject them to foreseeable and unreasonable risks of harm as a result of inadequate data security. *See also* Compl. ¶¶ 334-43 (allegations detailing duty).

Imposing such a duty on Equifax fulfills the underlying purposes of negligence law—compensation and deterrence—by placing the risk of loss on the

[1] The Court may also look to the common law of other jurisdictions in ascertaining a duty under Georgia law. *See, e.g.*, *Sims v. Am. Cas. Co.*, 131 Ga. App. 461, 470-73 (1974) (examining decisions from nine other jurisdictions). Other courts have routinely found a duty in similar circumstances. *See, e.g.*, *Brush v. Miami Beach Healthcare Grp. Ltd.*, 238 F. Supp. 3d 1359, 1365 (S.D. Fla. 2017); ("It is well-established that entities that collect sensitive, private data from consumers and store that data on their networks have a duty to protect that information."); *Sackin v. TransPerfect Global, Inc.*, 278 F. Supp. 3d 739, 747-48 (S.D.N.Y. 2017); *Hapka v. CareCentrix, Inc.*, 2016 WL 7336407, at *5 (D. Kan. Dec. 19, 2016).

only entity with the ability to prevent that loss. Absent a duty to protect consumers' data, Equifax has a strong incentive to cut corners and, as its CEO admitted, fail to live up to its responsibility for safeguarding confidential information while consumers who have no ability to protect themselves are forced to bear the costs. On the other hand, by imposing a duty, Equifax and other CRAs are incentivized to implement adequate security measures to avoid having to pay damages to those who are injured and, as a result, avert harm to consumers.[2]

Brushing aside Plaintiffs' detailed allegations related to its knowledge and the cases imposing a duty to safeguard personal information under similar circumstances, Equifax argues that *McConnell v. Dep't of Labor*, 345 Ga. App. 669, 676 (2018), *cert. pending*., Nos. S18C1316 and S181317 (Ga. May 31, 2018), compels this Court to reject *Arby's* and *Home Depot*. It urges the Court to instead

[2] The existence of a legal duty involves the "question of whether the defendant is under any obligation for the benefit of the particular plaintiff" and represents "an expression of the sum total of those considerations of policy which lead the law to say that the plaintiff is entitled to protection." W. Prosser and W. Keeton, *Law of Torts*, § 53 at 356, 358 (5th ed. 1984). Those policy considerations discussed in the text above support imposing a legal duty on Equifax. Further, federal public policy incorporated in Section 5 of the FTC Act, as discussed below, establishes a corporate duty to protect sensitive personal information, adding additional support to recognizing a common law duty under Georgia law. *See Pulte Home Corp. v. Simerly*, 322 Ga. App. 699, 705-06 (2006) ("violations of federal statutes and regulations support [a] claim of breach of legal duty in both traditional negligence and negligence per se actions").

hold that Georgia law imposes no duty *even if* Equifax "had warnings that its data security was inadequate and failed to heed them." *Contra Home Depot*, 2016 WL 2897520, at *4; *see* Mot. 24-32. That reading of *McConnell* is apt only to those willing to blind themselves to the circumstances of that particular case and traditional negligence principles applied by Georgia courts for decades.

In *McConnell*, an employee of a state agency mistakenly e-mailed sensitive information of over 4,000 Georgians to 1,000 recipients. In the first of two appellate decisions, the Georgia Court of Appeals held that Georgia's personal identity protection statute did not serve as the source of a statutory duty (for negligence purposes) to safeguard the personal information of those affected, the release of which was an unforeseeable event. *McConnell v. Dep't of Labor*, 337 Ga. App. 457, 458-63 (2016) (hereinafter *McConnell I*), *vacated*, 302 Ga. 18 (2017). In round two, the appeals court adhered to its initial decision after determining it had jurisdiction to hear the case. 345 Ga. App. at 675 (hereinafter *McConnell II*).

Notably, in *McConnell I*, the court itself distinguished *Home Depot* on the facts: "the district court found a duty to protect the personal information . . . in the context of allegations that the defendant failed to implement reasonable security measures . . . [despite] multiple warnings . . . and even took affirmative steps to

stop its employees from fixing known security deficiencies." 337 Ga. App. at 461 n.4. By comparison, the state court acknowledged, "There are no such allegations in this case." *Id*. Likewise, *Arby's*, decided after *McConnell I*, concluded that "*Home Depot* is not expressly inconsistent with *McConnell* because the facts are *starkly different*." 2018 WL 2128441, at *6 (emphasis added). For example, *Arby's* noted: "There were . . . no similar allegations of known security deficiencies in *McConnell*," or "any allegations that the action of the agency employee in 'inadvertently' emailing the spreadsheet containing the information was foreseeable." *Id*. (citing *McConnell I*, 337 Ga. App. at 458 n.1 & 459 n.4).

These factual differences regarding the foreseeability of the harm are the *sine qua non* of the duty and negligence analysis. "Neither duty nor negligence exists in a vacuum—they are entirely dependent upon circumstances involving others or their property." *Underwood v. Select Tire, Inc.*, 296 Ga. App. 805, 809 (2009) (quoting *Sims*, 131 Ga. App. at 468). To ascertain whether a legal duty exists, Georgia courts ask whether the circumstances in question were foreseeable: "Negligence is predicated on what should be anticipated, rather than on what happened, because one is not bound to anticipate or foresee and provide against what is unlikely, remote, slightly probable, or slightly possible." *Amos v. City of Butler*, 242 Ga. App. 505, 506 (2000). "[T]he legal duty to exercise ordinary care

arises from the foreseeable unreasonable risk of harm from such conduct." *Id.*; *see also, e.g.*, Restatement (Second) of Torts, Div. 2, Ch. 12, Topic 4, Scope Note (engrained in the law is the proposition that in performing "act[s] which affect[] the interests of another, there is a duty not to be negligent with respect to the doing of the act.").

Applying these principles, Georgia courts hold that a duty to protect against a third person's criminal act exists when there is "reason to anticipate" the criminal act. *Bradley Ctr., Inc. v. Wessner*, 250 Ga. 199, 202 (1982). "[W]ithout foreseeability that a criminal act will occur," however, "no duty . . . to exercise ordinary care to prevent that act arises." *Days Inns of Am., Inc. v. Matt*, 265 Ga. 235, 235 (1995) (holding prior robbery created triable issue as to whether hotel had duty to exercise ordinary care to guard patrons against risks posed by similar criminal activity). Thus, for example, in premises liability cases—a context "peculiarly similar" to data breach, *Arby's*, 2018 WL 2128441, at *4—Georgia courts hold a proprietor has a duty to use ordinary care to protect customers against the risk posed by foreseeable criminal activity. *Id*. (collecting Georgia cases).

Given the critical factual differences between the cases, Equifax is wrong that *McConnell II* conflicts with *Home Depot* or *Arby's*. Mot. 24. There were simply no allegations in *McConnell* that the state agency should have anticipated

the inadvertent disclosure of personal information by its employee. *Arby's*, 2018 WL 2128441, at *6. By comparison, in this case, as in *Home Depot* and *Arby's*, there are detailed, plausible, allegations that the data breach was foreseeable, triggering a duty to exercise reasonable care. *Arby's*, 2018 WL 2128441, at *5; *Home Depot*, 2016 WL 2897520, at *4.

Nor is Equifax correct that *McConnell* disavows *Wessner*'s holding that a duty arises when there is "reason to anticipate" a criminal act that would cause unreasonable harm to another. Mot. 29-32. *Arby's* concluded that any language to this effect in *McConnell I* is both dicta and unpersuasive stating: "any implication in [*McConnell I*] that the general duty of care owed to others does not apply outside the context of the specific facts in *Wessner* is misplaced" because *Wessner* itself explicitly recognized "there are cases such as this, however, in which the intervening criminal acts may be foreseeable." *Id*. (quoting *Wessner*, 250 Ga. at 202). The Georgia Court of Appeals must have taken this point to heart because, in *McConnell II*, the court dropped this dicta entirely. *See* 345 Ga. App. 669.

McConnell is not the only case Equifax misreads. Equifax claims that *Albany Urology Clinic, P.C. v. Cleveland*, 272 Ga. 296 (2000) suggests the Georgia Supreme Court would not recognize a duty here. Mot. 28. *Albany Urology*, however, did not concern a data breach, but a claim against a physician

whose illegal drug use allegedly led to unnecessary surgery. The court held against the plaintiff because it was unwilling to create an exception to a common-law evidentiary rule or recognize a new cause of action for "non-disclosure of a life factor by a professional." *See* 272 Ga. at 298-300. That result thus was driven by policy considerations not relevant in this case, *id.* at 301-03; and significantly the patient was not left without a remedy. *Id*. at 300 (patient had "full and adequate remedy for [his] injuries" under the law of professional negligence).

In contrast, Plaintiffs are not asking this Court to recognize a "new" tort, but rather to apply "traditional tort principles of negligence to the facts of this case." *Wessner*, 250 Ga. at 202; *see Arby's*, 2018 WL 2128441, at *7 (rejecting an argument that imposing a duty to guard against the risk of a foreseeable data breach is the equivalent of judicially creating a new cause of action). And, unlike in *Albany Urology*, social policy supports a duty here, otherwise CRAs could continue "to use outdated security measures and turn a blind eye to the ever-increasing risk of cyberattacks, leaving consumers with no recourse to recover damages." *Home Depot*, 2016 WL 2897520, at *4; *accord Arby's*, 2018 WL 2128441, at *4-5.[3]

[3] Equifax argues that a court must "limit" a tortfeasor's responsibility to a "controllable degree" and, as a result, there should be no duty to prevent a

Equifax also misreads *Wells Fargo Bank, N.A. v. Jenkins*, 293 Ga. 162 (2013), arguing the decision "indicat[es] that [no duty] exists at Georgia common law." Mot. 28. *Jenkins*, however, held only that duties imposed by the Gramm–Leach–Bliley Act, 15 U.S.C. § 6801(a), do not give rise to a cause of action for negligence under O.C.G.A. § 51-1-6. *Id.* at 165 n.4 ("the question of a legal duty under the cited provision of the GLBA is the linchpin of the Court of Appeals holding at issue and is the precise question on certiorari"). There is a reason no court has read *Jenkins* more expansively as Equifax urges; the case simply does not decide this particular issue. *See Arby's*, 2018 WL 2128441, at *4 ("there are no Georgia appellate cases that have considered negligence claims in a large data breach involving a third party criminal hacker").

Lastly, Equifax divines a rule that there must be a "direct relationship" between the tortfeasor and a victim for a duty to exist and argues such a

---

foreseeable data breach because that would "create an almost infinite universe of potential plaintiffs." Mot. 29. This perverse argument is akin to the "too big to fail" rationale that lead to the Great Recession, suggesting a company should have no duty to do anything so long as the foreseeable result of its inaction is massive harm to tens of millions of victims. In fact, the need for a duty in such circumstances is even more critical to ensure that companies have an incentive to spend the money needed to prevent the harm in the first place, rather than allowing them to shift the expense of failing to do so to innocent third-parties. That result serves the basic purposes of tort law and, from a global perspective, makes sense because the cost to Equifax of having adequate data security is a small fraction of the damage it has imposed on Plaintiffs and the consumer credit system.

relationship is lacking here. Mot. 30 & n.8. This argument fails on the facts and the law. The facts: Plaintiffs do have a relationship with Equifax as the data at issue pertains to them and is fundamental to Equifax's business and Plaintiffs' participation in daily economic life. *See In re Syngenta AG MIR 162 Corn Litig.*, 131 F. Supp. 3d 1177, 1191 (D. Kan. 2015) (seller of genetically modified crop seeds owed a duty to farmers with whom it had no preexisting relationship because all parties were "participants in an inter-connected market"). Certainly the nature of the relationship, however characterized, is such that Equifax cannot credibly argue it was unforeseeable Plaintiffs would suffer harm from a data breach, the only logical reason why any relationship is necessary. As for the law, Equifax's cases are inapposite. Mot. 30 n.8. All represent failed attempts to hold medical professionals liable for harm their patients caused to third parties, *see id.*, circumstances that are not analogous to those alleged here.

2. Equifax Inappropriately Seeks To Hide Behind The Economic Loss Rule.

Equifax blithely ignores the fact that this Court has twice rejected the application of the economic loss rule to data breach cases, holding that the rule does not apply when there is an "independent duty of care." *See Arby's*, 2018 WL 2128441, at *12-14; *Home Depot*, 2016 WL 2897520, at *3-4. As discussed above and in this Court's previous decisions, the duty to safeguard consumers' personal

information in the face of a foreseeable security threat is a duty independent of any contract. *See Home Depot*, 2016 WL 2897520, at *4; *Arby's*, 2018 WL 2128441, at *5. Plaintiffs' claims thus are not barred by the economic loss rule.

3. All Plaintiffs Allege Legally Cognizable Harms.

The injury requirement in the data breach context is usually considered in the context of Article III standing. However, Equifax does not dispute standing and instead argues that Plaintiffs fail to plead "legally cognizable harms" under Georgia law. In so doing, Equifax presumably seeks to avoid the emerging body of law holding that the harms alleged here create standing, but its effort is unavailing. *See Dieffenbach v. Barnes & Noble, Inc.*, 887 F.3d 826, 828 (7th Cir. 2018) ("To say that the plaintiffs have standing is to say that they have alleged injury in fact, and if they have suffered an injury then damages are available."). In other words, the injuries alleged here "can justify money damages, just as they support standing." *Id*. Consequently, Equifax cannot avoid adverse case law on standing simply by re-framing the issue, and Equifax's failure to challenge standing is a tacit admission that Plaintiffs sufficiently allege injury.[4]

[4] To the extent Equifax argues that Plaintiffs do not satisfy state-court pleading requirements, "in federal court it is the federal rules that determine what must be in a complaint." *Barnes & Noble*, 887 F.3d at 828.

Contrary to Equifax's claim, each Plaintiff has alleged injury in one or more of the following ways: (1) spending time and incurring out-of-pocket loss addressing issues relating to identity theft and fraud; (2) purchasing credit monitoring and credit freezes to mitigate possible harm; (3) monitoring financial accounts; (4) experiencing a decline in credit scores, which jeopardizes their borrowing ability and causes other problems; (5) lost opportunity costs, unauthorized withdrawals from their accounts, and the loss of value of personal information; and (6) imminent risk of future harm. *See* Compl. ¶¶ 11-108; 235-43.

Numerous courts, including this one, hold such allegations are sufficient. *See, e.g.*, *Home Depot*, 2016 WL 2897520, at *3; *Arby's*, 2018 WL 2128441, at *11 (monetary losses related to fraudulent charges, theft of personal financial information, and costs associated with detection and prevention of identity theft sufficient); *Barnes & Noble*, 887 F.3d at 828 ("[T]he value of one's own time needed to set things straight is a loss from an opportunity-cost perspective."); *In re Anthem, Inc. Data Breach Litig.*, 2016 WL 3029783, at *14-15 (N.D. Cal. May 27, 2016) (plaintiffs "sufficiently pleaded damages for Loss of Value" of personal information); *Resnick v. AvMed, Inc.*, 693 F.3d 1317, 1323 (11th Cir. 2012); *Hutton v. Nat'l Bd. of Examiners in Optometry, Inc.*, 892 F.3d 613, 622, 623, n.9 (4th Cir. 2018) (costs of taking mitigating measures, drop in credit score, and time

lost dealing with repercussions of data breach constitute injuries); *Attias v. Carefirst, Inc.*, 865 F.3d 620, 627 (D.C. Cir. 2017), *cert. denied*, 138 S. Ct. 981 (2018); *In re Yahoo! Inc. Customer Data Sec. Breach Litig.*, 2017 WL 3727318, at *16 (N.D. Cal. Aug. 30, 2017).[5]

Ignoring this body of case law, including *Arby's* and *Home Depot*, Equifax nonetheless argues that Plaintiffs have not alleged any legally cognizable injuries. Equifax's arguments are unavailing for many reasons. *First*, the cases on which it relies are easily distinguishable. In *Finnerty v. State Bank & Trust Co.*, 301 Ga. App. 569 (2009), the plaintiff alleged an *invasion of privacy* claim premised on the public disclosure of his Social Security number in a court filing and the court found the plaintiff was unlikely to suffer harm because he "failed to allege that anyone actually viewed his social security number." *Id.* at 571-72. Similarly, in

[5] *Collins v. Athens Orthopedic Clinic* recently upheld dismissal of a data breach case where the plaintiffs alleged potential future costs associated with lifetime credit monitoring or credit freezes, but no current out of pocket losses tied to the breach. 815 S.E.2d 639 (Ga. App. 2018). The opinion is not binding precedent. Ga. Ct. App. R. 33.2(a)(1). Regardless, it is inapplicable. Because the *Collins* plaintiffs alleged only an "increased risk of harm," the court found that future costs for "credit monitoring and other precautionary measures" were not recoverable, limiting the decision to the "facts before us." *Id.* In so doing, the Court distinguished *Arby's* and *Resnick* because in those cases the plaintiffs pled "costs associated with actual data theft" and actual "financial injury" as a result of the breaches. 815 S.E.2d at 639. Plaintiffs here plead financial injury.

Rite Aid of Georgia, Inc. v. Peacock, a decision relating to class certification, there was no allegation of misuse or likely misuse of the confidential information. 315 Ga. App. 573, 576-77 (2012). Likewise, *Randolph v. ING Life Ins. & Annuity Co*., involved the theft of a laptop containing employees' personal information but "there [was] no evidence that the burglary was undertaken for the specific purpose of obtaining the information on the laptop" as opposed to the laptop itself. 973 A.2d 702, 704-05 n.2 (D.C. 2009). Plaintiffs allege here, by contrast, that their personal information has *already* been misused.

Second, Equifax wrongly denies that a risk of future harm is legally cognizable. As the Supreme Court has recognized, future harm is a cognizable injury when it is either "certainly impending" or the risk is "substantial." *Susan B. Anthony List v. Driehaus*, 134 S. Ct. 2334, 2341 (2014). Plaintiffs allege both an impending and substantial risk of future harm, which only makes sense since the compromised information was stolen by criminals in order to misuse it. Such allegations are sufficient. *See, e.g., Attias*, 865 F.3d at 629 ("a substantial risk of harm exists already, simply by virtue of the hack and the nature of the data that the plaintiffs allege was taken"); *Galaria v. Nationwide Mut. Ins. Co.*, 663 F. App'x 384, 387-89 (6th Cir. 2016) ("There is no need for speculation where [p]laintiffs allege that their data has already been stolen and is now in the hands of ill-

intentioned criminals"). To the extent Equifax questions whether Plaintiffs' mitigation expenses were necessary or recoverable, those are jury issues. *See Lewert v. P.F. Chang's China Bistro, Inc.*, 819 F.3d 963, 969 (7th Cir. 2016) ("[A]ll class members should have the chance to show that they spent time and resources tracking down the possible fraud, changing automatic charges, and replacing cards as a prophylactic measure."); *Arby's*, 2018 WL 2128441, at *11 n.12 ("[I]n the Court's view, a consumer's time and effort to remediate the effects of a breach is not an abstract notion of actual damage and one that is susceptible to proof and valuation by a jury.").

Third, Equifax wrongly claims that Plaintiffs victimized by credit card fraud failed to plead "a cognizable injury at all—much less one resulting from the Equifax data breach." Mot. 19-20. All such Plaintiffs aver that they used their credit or debit cards with Equifax in previous transactions, they were notified directly by Equifax that their cards had been compromised, and fraudulent charges were made on their cards in the aftermath of the breach. Compl. ¶¶ 26, 33, 60. These statements are sufficient. *See, e.g.*, *Home Depot*, 2016 WL 2897520, at *3.[6]

[6] The cases cited by Equifax are inapposite. In *Provost v. Aptos, Inc.*, the court initially dismissed a claim alleging injury based on a single unauthorized charge almost two years earlier, "with no additional fraudulent charges since then" and the absence of "any information about this charge other than its existence, upon

Plaintiffs need not allege that they were never reimbursed for the fraudulent charges. *See, e.g.*, *Resnick v. AvMed, Inc.*, 693 F.3d 1317, 1324 (11th Cir. 2012) (finding as specious defendant's argument that plaintiffs did not suffer from cognizable losses because they did not allege "unreimbursed losses"); *Smith v. Triad of Alabama, LLC*, 2015 WL 5793318, at *9 (M.D. Ala. Sept. 29, 2015); *Barnes & Noble*, 887 F.3d at 828. In any case, payment card fraud is a form of identity theft which, in and of itself, "constitute[s] a concrete and particularized injury." *Attias*, 865 F.3d at 627.

Finally, Plaintiffs also seek recovery of nominal damages. *See* Compl. ¶¶ 347, 354, 381, 408, 416, 591. Georgia's Supreme Court has explained that:

> Nominal damages come into play when an injured party establishes a breach of contract, but is unable to prove actual damages.
>
> [C]ase law makes clear nominal damages are awarded: (1) *where no actual damage flows from the injury*; or (2) where the violation of a right is shown, substantial damages claimed, and some actual loss proved, and yet the damages are not susceptible of reasonable certainty of proof as to their extent.

King v. Brock, 282 Ga. 56, 57 (2007) (emphasis added); *see also Mobley v. Murray Cty.*, 178 Ga. 388, 394 (1934) ("[R]ight to sue would have arisen for recovery of

---

information and belief." 2018 WL 1465766, at *3, 5-6 (N.D. Ga. Mar. 12, 2018). Similarly, the court in *Torres* initially dismissed the claim because the single plaintiff did not allege any actual loss, but allowed the case to proceed after new plaintiffs were added who alleged late fees and loss of cash-back rewards. *Torres v. Wendy's Co.*, 195 F. Supp. 3d 1278, 1285 (M.D. Fla. 2016).

nominal damages, at least, for the breach of the bank's implied contract"); O.C.G.A. § 13-6-6. This concept is not limited to contract actions, but includes alleged torts. *See* O.C.G.A. § 51-12-4; *Ackley v. Strickland*, 173 Ga. App. 784, 786 (1985) (plaintiff conceded lack of evidence of specific damage; nominal damages still recoverable as "[the] law *infers* some damage from the invasion of a property right and if no evidence is given of any particular amount of loss, declares the right by awarding what it terms nominal damages"); *City of Greensboro v. McGibbony*, 93 Ga. 672, 677-78 (1894) ("the plaintiff was entitled to at least nominal damages for the loss of his time"); *Velez v. Bethune*, 219 Ga. App. 679, 681 (1995) (Beasley, J., specially concurring) ("The fact that there may be little or no actual damages does not govern whether there is a compensable tort.").

4. Plaintiffs Allege The Equifax Breach Is The Proximate Cause Of Their Injuries.

Throughout its brief, Equifax contends Plaintiffs have not alleged that their harms are "proximately tied" to the breach. *See* Mot. 20-23. But each Plaintiff has explicitly—and plausibly—alleged proximate causation. All Plaintiffs verified through the Equifax website that their personal information was compromised; detail the various forms of harm they have suffered, including incurring the cost of freezing their credit as Equifax told them to do; and assert this harm was a direct result of the breach. Compl. ¶¶ 11-108, 282-94. Whether these allegations can be

proven is an issue of fact for summary judgment or trial. *See Redmon v. Daniel*, 335 Ga. App. 159, 166 (2015) ("[Q]uestions of causation are normally for the jury" to resolve); *Hite v. Anderson*, 284 Ga. App. 156, 158 (2007) (at motion to dismiss stage, plaintiffs must merely allege proximate cause).

There is no requirement, as Equifax argues, that a Plaintiff must allege "her PII was not stolen in other data breaches." Mot. 21. The argument that a victim of a previous data breach cannot be further victimized by a subsequent breach has been rejected time and again. *See, e.g.*, *Yahoo!*, 2017 WL 3727318, at *19 (existence of other data breaches does not defeat causation); *Remijas v. Neiman Marcus Group, LLC*, 794 F.3d 688, 697 (7th Cir. 2015) ("The fact that . . . some other store might have caused the plaintiffs' private information to be exposed does nothing to negate the plaintiffs' standing to sue."); *In re Anthem, Inc. Data Breach Litig.*, 162 F. Supp. 3d 953, 988 (N.D. Cal. 2016) (rejecting the argument because it would "create a perverse incentive for companies: so long as enough data breaches take place, individual companies will never be found liable."). Even assuming some Plaintiffs' data was previously stolen, whether the harm they allege here resulted from the earlier breach rather than this one is quintessentially a fact question. *See Attias*, 865 F.3d at 629.

Finally, Equifax cannot avoid liability for its own conduct by blaming the hackers and asserting the breach was unforeseeable because it resulted from criminal activity. Mot. 21-22. Equifax's assertion is not grounds for dismissal—it raises an issue for the jury. *See Sturbridge Partners, Ltd. v. Walker*, 267 Ga. 785, 786 (1997) (foreseeability is for the jury). An intervening criminal act does not insulate a defendant from liability as a matter of law where, as here, "it is alleged that the defendant had reason to anticipate the criminal act." *Atlantic C. L. R. Co. v. Godard*, 211 Ga. 373, 377 (1955); *Wessner*, 250 Ga. at 202 (same); *Landis v. Rockdale County*, 206 Ga. App. 876, 881 (1992) (same). The Court should therefore reject Equifax's reliance on *Andrews v. Kinsel*, 114 Ga. 390 (1901), which did not involve any allegations that the criminal act was foreseeable, and instead apply longstanding black-letter law that supports Plaintiffs' position. *See, e.g.*, *Arby's*, 2018 WL 2128441, at *3-4 (rejecting the argument that hackers are an unforeseeable intervening cause).

B. Plaintiffs Adequately Allege Negligence Per Se.

Under Georgia law, violation of a statute or regulation that serves as a standard of conduct constitutes negligence per se. *See, e.g.*, *Pulte Home Corp.*, 322 Ga. App. at 705-06. A plaintiff must show that he or she is within the class of persons the statute was intended to protect and the statute was intended to protect

against the harm suffered. *See, e.g., Amick v. BM & KM, Inc.*, 275 F. Supp. 2d 1378, 1382 (N.D. Ga. 2003).

Plaintiffs assert a negligence per se claim premised on Section 5 of the FTC Act, 15 U.S.C. § 45, which prohibits unfair or deceptive trade practices.[7] The failure to maintain reasonable data security measures to safeguard confidential consumer information is an unfair practice prohibited by the Act. *See, e.g., F.T.C. v. Wyndham Worldwide Corp.*, 799 F.3d 236, 240 (3d Cir. 2015). Plaintiffs allege Equifax violated Section 5 by not having reasonable data security, they are within the class the section was intended to protect, and the section was meant to protect against the harm that occurred. Compl. ¶¶ 350-54. Such allegations properly state a claim for negligence per se under Section 5, as at least three courts have held in other data breach cases. *See, e.g., Home Depot*, 2016 WL 2897520, at *4; *Arby's*, 2018 WL 2128441, at *8-9; *First Choice Fed. Credit Union v. Wendy's Co.*, 2017 WL 9487086, at *4 (W.D. Pa. Feb. 13, 2017), *report and recommendation adopted*, 2017 WL 1190500 (W.D. Pa. Mar. 31, 2017). Ignoring these cases, Equifax argues the claim should be dismissed for four reasons. None has merit.

[7] Plaintiffs also state negligence per se claims predicated on various state statutes modeled after Section 5, such as the Georgia Fair Business Practices Act. The same rationale that supports Plaintiffs' claim under Section 5 supports the additional state statutory claims.

First, Equifax argues Section 5 is "not specific enough" to create a statutory duty. Mot. 35. But this argument was summarily rejected in *Arby's*, *Home Depot*, and *Wendy's*, *see Arby's*, 2018 WL 2128441, at *8, and Equifax does not even attempt to explain why those decisions are wrong. Further, "two circuit courts have expressly held that 'unfair' or 'deceptive' trade practices under Section 5 of the FTCA fairly encompass the failure to provide adequate data security measures to protect consumer financial data from threat of hacking." *Id*. (summarizing *Wyndham*, 799 F.3d at 247 and *In re TJX Cos. Retail Sec. Breach Litig*., 564 F.3d 489, 498 (1st Cir. 2009)).[8]

Second, Equifax misreads the Eleventh Circuit's decision in *LabMD, Inc. v. F.T.C.*, 894 F.3d 1221 (11th Cir. 2018). According to Equifax, *LabMD* holds that a practice must violate clear policies established under the common law to be unfair under Section 5 and, because the common law imposes no duty to maintain reasonable data security, Equifax could not have violated Section 5. However, the

[8] In arguing that only a specific duty, rather than a generalized standard of conduct such as the requirement to maintain reasonable data security, can support a claim for negligence per se, Equifax also ignores contrary Georgia law. As the Georgia Supreme Court has held, "Where a statute provides a general rule of conduct, *although only amounting to a requirement to exercise ordinary care*, the violation thereof is negligence as a matter of law, or negligence per se." *Teague v. Keith*, 214 Ga. 853, 853-54 (1959) (emphasis added) (noting for example that a negligence per se claim can be based on statutes prohibiting a driver from driving at a "speed greater than is reasonable").

Eleventh Circuit did not hold the common law imposes no such duty, but in fact assumed that a common law duty exists, citing the Restatement (Second) of Torts. *See id.* at 1231. The court vacated the FTC's order at issue because the order was too vague to be enforced—an issue not presented here—not because inadequate data security cannot be regulated under Section 5. *See id*. at 1236-37.[9]

Third, Equifax argues Plaintiffs have no valid claim under Section 5 because the FTC has not adopted a formal regulation regarding data security, but only issued directives through publications and enforcement orders. But there is no requirement that the FTC issue formal regulations to designate a practice as unfair. *See id.* at 1232 ("Because Congress thought impossible the task of legislating a comprehensive list of unfair acts or practices, it authorized the Commission to establish unfair acts or practices through case-by-case litigation."). Moreover, Georgia law does not require that a governmental directive be expressed in a

[9] Equifax's argument that inadequate data security is not an unfair practice under Section 5 rests on the assertion Georgia common law imposes no duty on Equifax to safeguard confidential information, which is incorrect for the reasons discussed above. Regardless, Section 5 is a federal statute and, as such, applies uniformly throughout the nation and preempts contrary state law. Accordingly, the *LabMD* court did not examine the law in the defendant's home state, but rather the common law generally as expressed in the Restatement. 894 F.3d at 1231. To adopt Equifax's rationale would mean that Section 5 must be construed differently depending on the state in which the conduct at issue occurred, a novel proposition for which Equifax provides no authority.

statute or regulation to be enforceable. *Jenkins*, 293 Ga. at 165 (recognizing that negligence per se can be based on a common law principle or any "regulation, *directive*, or *standard*" authorized by law) (emphasis added).

Finally, Equifax conflates implied rights of action with negligence per se. Mot. 36. Georgia law is clear that negligence per se claims are cognizable even if the predicate statute contains no private right of action. *See Pulte Home Corp.*, 322 Ga. App. at 707; *see generally* O.C.G.A. § 51-1-6.

C. Plaintiffs State A Claim Under The Georgia Fair Business Practices Act.

The GFBPA provides a remedy to persons harmed by "unfair or deceptive practices." O.C.G.A. §§ 10-1-391(a); 399(a). As a remedial statute, it "is to be liberally construed and applied to promote its underlying purposes and policies, which are to protect consumers." *Georgia Receivables, Inc. v. Welch*, 242 Ga. App. 146, 146 (2000). "Except in plain and indisputable cases, the question of whether a particular act or omission, or a series thereof, constitutes unfair or deceptive acts or practices within the meaning of O.C.G.A. § 10-1-393 generally is for jury resolution." *Regency Nissan, Inc. v. Taylor*, 194 Ga. App. 645, 648 (1990).

Plaintiffs have plausibly stated all elements of a GFBPA claim.[10] *See* Compl. ¶¶ 355-80. Equifax's arguments to the contrary lack merit.

First, Equifax again marginalizes *Arby's*, which was decided after *McConnell* and held that data breach victims have a claim under the GFBPA. *See In re Arby's Rest. Grp. Inc. Litig.*, 2018 WL 3549783, at *4 (N.D. Ga. June 28, 2018). Equifax also misconstrues *McConnell*, which says only that the Georgia statutory prohibition on displaying Social Security numbers (O.C.G.A. § 10-1-393.8) and the data breach notification statute (O.C.G.A. § 10-1-910) are not the basis of a general tort duty. *McConnell II*, 345 Ga. App. at 676-79. Unlike Plaintiffs, the *McConnell* plaintiffs did not assert a GFBPA claim. *See* Br. of Appellant, *McConnell v. Dep't of Labor*, 2017 WL 5194734, at *24. Thus, *McConnell* did not consider the issue presented here. Nor did it discuss the impact of judicial and agency interpretations of Section 5, which are incorporated into the GFBPA by the terms of the statute, O.C.G.A. § 10-1-391(b). The same analysis

[10] Equifax argues for a heightened pleading standard under the GFBPA, arguing Plaintiffs "have not pleaded that they read and relied on any representations made by Equifax." Mot. 40 n.12. But that is more than is required, as "logic dictates that plaintiffs alleging misconduct by omission or passive conduct . . . will be less able to specify the details of the wrongdoing . . . ." *In re Arby's*, 2018 WL 3549783, at *2, 4 (rejecting heightened pleading standard under GFBPA).

applies to Plaintiffs' claim under Georgia's Uniform Deceptive Trade Practices Act. *See* Mot. 64.

Second, Equifax argues that Plaintiffs could not have relied on its misrepresentations and omissions because Equifax collects most consumer data from third parties and because Plaintiffs could not opt out of Equifax's data collection practices. Mot. 39-40. This argument ignores Plaintiffs' allegations that Equifax has a special role in the consumer economy in which CRAs are authorized to gather Plaintiffs' confidential information and, in highly regulated circumstances, disseminate that information for the common good.[11] Compl. ¶¶ 1, 122-23, 125-27, 134-36.

The reality is that all of the actors in the consumer economy—including Plaintiffs, data furnishers, and regulators—relied to their detriment on Equifax's actions. By misrepresenting the truth regarding its commitment to data security and failing to disclose that its existing security measures were virtually non-existent, Equifax deprived the marketplace, including Plaintiffs, of critical information

[11] Equifax itself seemingly acknowledges this special role, explaining, "We have built our reputation on our commitment to deliver reliable information to our customers . . . and to protect the privacy and confidentiality of personal information about consumers." Compl. ¶ 151. And the company did so again in apologizing for the breach, stating: "Equifax was entrusted with Americans' private data and we let them down." *Id.* ¶ 278.

needed to make informed decisions. Had the truth been known, Plaintiffs and the other actors could have taken protective action, such as refusing to do business with Equifax and those who furnished data to Equifax, or otherwise adjusting their behavior.[12] These allegations of reliance thus are sufficient at the pleading stage.

Regardless, Plaintiffs need not plead reliance to state a GFBPA claim based on omissions as opposed to misrepresentations, as Plaintiffs have done. Reliance is not an express statutory element. *See* O.C.G.A. §§ 10-1-393 & 10-1-399(a); *Johnson v. GAPVT Motors, Inc.*, 292 Ga. App. 79, 84 (2008) (elements are "violation of the Act, causation, and injury"). While Georgia courts, writing in broad strokes, have characterized the GFBPA as requiring reliance, those cases turn on affirmative deception or misrepresentation theories, not omissions. *See, e.g.*, *Tiismann v. Linda Martin Homes Corp.*, 281 Ga. 137, 138 (2006) ("[H]e cannot show that he placed any reliance on LMH's allegedly deceptive *misrepresentation*") (emphasis added); *Zeeman v. Black*, 156 Ga. App. 82, 87 (1980) ("[A] claimant who alleges the FBPA was violated *as the result of a*

[12] That Equifax's misrepresentations and omissions may have triggered reliance by third-parties and those third-parties would have forced remedial action is immaterial at this stage. Plaintiffs allege that Equifax acted wantonly and willfully. *Id.* ¶ 373. "Where the misrepresentation is willfully made, privity is not necessary to give rise to the cause of action." *Robert & Co. Assocs. v. Rhodes-Haverty P'ship*, 250 Ga. 680, 681 (1983) (citing O.C.G.A. § 51-6-2).

misrepresentation must demonstrate . . . the reliance upon the alleged misrepresentation.") (emphasis added). The holdings in those cases make sense. Without proof of reliance, a plaintiff cannot establish that the misrepresentation made any difference and thus cannot prove causation.

In contrast, under an omission theory, to prove that the omission mattered—and thus establish causation—logically a plaintiff need not show reliance upon or even awareness of the fact that the defendant failed to disclose the truth. The critical question is whether the plaintiff would have acted differently had the truth been disclosed. *See Skeen v. BMW of N. Am., Ltd. Liab. Co*., 2014 WL 283628, at *11 (D.N.J. Jan. 24, 2014) (denying dismissal of part of GFBPA claim based on fraudulent omissions); *accord In re Anthem*, 2016 WL 3029783, at *35 ("Reliance can be proven in a fraudulent omission case by establishing that had the omitted information been disclosed, the plaintiff would have been aware of it and behaved differently."); *In re Adobe Sys. Privacy Litig*., 66 F. Supp. 3d 1197, 1231 (N.D. Cal. 2014) (same). Plaintiffs allege just that—namely, had it been known that Equifax was unwilling or unable to secure confidential consumer data, they and other economic actors would have made different decisions, required Equifax to clean up its act, or forced Equifax out of business.

Similarly, there is no logical reason to require reliance when, as here, Plaintiffs allege Equifax committed "unfair acts and practices" separate and apart from acts of deception. Compl. ¶ 361; *see In re Arby's*, 2018 WL 3549783, at *3-4 (recognizing that under GFPBA a plaintiff "may proceed under an 'unfairness' theory," distinct from a "deception" theory). An "unfair" act is not necessarily deceptive. For example, a loan shark who imposes a usurious interest rate or a bank that steals money from a consumer's account by charging an improper fee engages in an unfair practice, even if the interest rate or fee is disclosed. To require reliance in such cases would deprive the victim of any remedy and thus gut GFBPA's unfairness prong. For that reason, courts in other states have construed similar statutes as not requiring reliance in unfair practice cases. *See Yue v. Conseco Life Ins. Co.*, 282 F.R.D. 469, 476-77 (C.D. Cal. 2012) ("[R]elief under the [California UCL] is available without individualized proof of deception, reliance and injury" where plaintiff pursues "unlawful" or "unfair" prongs); "Right to Privacy Action Under State Consumer Protection Act – Preconditions to Action," 117 A.L.R.5th 155, § 10[b]. The same logic applies here.

Third, Equifax asserts that class actions are not permitted under the GFBPA—and other state statutes, Mot. 41 n.14—but in the same breath acknowledges that Rule 23 overrides state statutory restrictions on representative

actions. *Lisk v. Lumber One Wood Preserving, LLC*, 792 F.3d 1331 (11th Cir. 2015) (applying *Shady Grove Ortho. Assocs. v. Allstate Ins. Co.*, 559 U.S. 393 (2010)). Equifax's assertion thus fails. *See Arby's*, 2018 WL 2128441, at *19.

D. The Complaint Plausibly States a Claim of Unjust Enrichment.

Under Georgia law, the "essential elements" of a claim for unjust enrichment are "(1) a benefit has been conferred, (2) compensation has not been given for receipt of the benefit, and (3) the failure to so compensate would be unjust." *Clark v. Aaron's, Inc.*, 914 F. Supp. 2d 1301, 1309 (N.D. Ga. 2013). Plaintiffs satisfy each element, alleging that Equifax knowingly obtained a benefit when it received their personal information, did not compensate Plaintiffs, and should be required to return the benefit in accordance with equitable principles because of the company's wanton and willful misconduct. Compl. ¶¶ 382-391. These allegations state a claim for unjust enrichment. *See Arby's*, 2018 WL 2128441, at *17 (sustaining consumer plaintiffs' claim for unjust enrichment); *Sackin*, 278 F. Supp. 3d at 751-52 (employees stated claim for unjust enrichment in context of employer's data breach where employer was enriched at employees' expense "when it chose to cut costs by not implementing security measures to protect Plaintiffs' PII").

Equifax argues that only those Plaintiffs who *directly* provided information to Equifax conferred on it a benefit. But this argument ignores the interrelatedness of the credit reporting industry, which inherently relies on the transfer of consumer information to Equifax through data furnishers and other third parties under a statutory scheme in which Plaintiffs directly participate. Moreover, the stolen data pertains and belongs to Plaintiffs and would never have been given to Equifax *at all* if Equifax's lack of commitment to maintain its privacy were known. Compl. ¶ 386. Whether under these circumstances Equifax received a "direct" benefit thus is a question of fact that cannot be resolved at this stage. *See In re ConAgra Peanut Butter Products Liab. Litig.*, 2008 WL 2132233, at *3 (N.D. Ga. May 21, 2008).

Regardless, Georgia law does not limit unjust enrichment claims to direct benefits. *See Terrill v. Electrolux Home Products, Inc.*, 753 F. Supp. 2d 1272, 1290 (S.D. Ga. 2010); *compare Mullinax v. United Mktg. Grp., LLC*, 2011 WL 4085933, at *14 (N.D. Ga. Sept. 13, 2011) ("Whether Georgia law permits an unjust enrichment claim where the alleged benefit is conferred indirectly on a party appears to be an open question.") *with* Unjust Enrichment, Ga. Contracts Law and Litigation § 12:8 (2d ed.) (noting the "concept of privity may exist in *some* unjust enrichment actions") (emphasis added). Because Equifax undeniably was aware of

the benefit and the data it received pertained to Plaintiffs, whether the benefit was conferred directly or indirectly is a red herring of no consequence.

Equifax next argues that the "Contract Plaintiffs" do not have an unjust enrichment claim because they "explicitly allege" having contracts with Equifax. *See* Mot. 42. But while a plaintiff "cannot recover under both a breach of contract and unjust enrichment theory, a plaintiff may plead these claims in the alternative." *Arby's*, 2018 WL 2128441, at *17; *Fed. Ins. Co. v. Westside Supply Co.*, 264 Ga. App. 240, 248 (2003). Equifax disputes the existence of the alleged express or implied contracts. Consequently, it would be premature to dismiss the claim on this basis. *See Arby's*, 2018 WL 2128441, at *17.

Finally, Equifax argues that Plaintiffs' damages are limited to the reasonable value of the benefit conferred, and not the profits Equifax received from the use and sale of personal information. Mot. 43. However, these two concepts are not necessarily mutually exclusive, as the "benefit is measured from the standpoint of the person upon whom such benefits were conferred." *Zampatti v. Tradebank Int'l Franchising Corp.*, 235 Ga. App. 333, 340 (1998). At any rate, the determination of the amount of that gain is "uniquely" a jury question, not an issue to be decided on a motion to dismiss. *Watson v. Sierra Contracting Corp.*, 226 Ga. App. 21, 28 (1997).

II. PLAINTIFFS ADEQUATELY PLEAD CONTRACT CLAIMS.

A. Plaintiffs Allege That Equifax Breached An Express Contract.

Equifax's motion to dismiss the Contract Plaintiffs' claim for breach of express contract fails for several reasons. *First*, by its own terms, the Equifax Terms of Service and Product Agreement—the "express contract" Equifax contends governs these claims—"does not apply to . . . the Equifax Cybersecurity Incident announced on September 7, 2017." *See* Equifax Terms of Service and Product Agreement, *available at* https://bit.ly/2LVxNI0 ("Product Agreement"). Equifax's argument that the Product Agreement's merger clause excludes consideration of the Privacy Policy thus is flatly wrong. Further, the Product Agreement cited by Equifax is dated January 31, 2018—after the data breach and the conduct that led to this action. If any Product Agreement applies, it is one that was in effect at the time of the breach. Equifax has not submitted such an agreement at the motion to dismiss stage, and so Plaintiffs' allegations about the substance of their contract with Equifax remain uncontroverted.

Second, Plaintiffs have adequately pleaded the Privacy Policy is a contract that was formed when they purchased services from, or otherwise provided personal information to, Equifax, such as when they obtained their credit files, disputed entries, or froze their credit. Compl. ¶¶ 401, 405. Courts are admittedly

divided on whether privacy policies are standalone contracts, but the better-reasoned cases hold that they are. *See, e.g., In re Jetblue Airways Corp. Privacy Litig.*, 379 F. Supp. 2d 299, 325-27 (E.D.N.Y. 2005) ("stand-alone privacy statement" could form basis of contract between airline and customers who made flight reservations); *Meyer v. Christie*, 2007 WL 3120695, at *4 (D. Kan. Oct. 24, 2007) (privacy policy was impliedly part of bank's loan offer). If ever there is a case where a privacy policy should be construed a standalone contract, this is it. Equifax's entire business model revolves around collecting and selling sensitive information. When consumers provide such information to Equifax, the company receives valuable consideration and, by the very nature of the interaction, consumers reasonably expect their information will be protected.

Regardless of whether the Privacy Policy is a standalone contract, it was incorporated into Equifax's Terms of Use for its website:

> *Subject to the conditions described on the privacy page of this Web Site*, EQUIFAX shall have no obligation of any kind with respect to such Feedback and shall be free to use and distribute the Feedback to others without limitation.

Site Terms of Use, *available at* https://www.equifax.com/terms/ (emphasis added). The Privacy Policy, as a result, is enforceable through the Terms of Use. *See In re Anthem*, 2016 WL 3029783, at *10 (contract claim could be based on privacy policy that was incorporated into defendant's terms of service). Courts routinely

hold that such terms of use are binding contracts. *Snap-on Bus. Sols. Inc. v. O'Neil & Assocs., Inc.*, 708 F. Supp. 2d 669, 683 (N.D. Ohio 2010); *Walsh v. Microsoft Corp.*, 63 F. Supp. 3d 1312, 1320 (W.D. Wash. 2014). Cases that have held to the contrary generally involve businesses suing consumers, not vice versa as in this case. *Berkson v. Gogo LLC*, 97 F. Supp. 3d 359, 396 (E.D.N.Y. 2015) ("[C]ourts have been willing to enforce terms of use against corporations, but have not been willing to do so against individuals.").

Under Georgia law, "incorporation by reference is generally effective to accomplish its intended purpose where . . . the provision to which reference is made has a reasonably clear and ascertainable meaning." *Dan J. Sheehan Co. v. Ceramic Technics, Ltd.*, 269 Ga. App. 773, 777 (2004) (credit agreement providing that buyer would be bound by "sellers' terms and conditions" was sufficient to incorporate separate sheet of terms and conditions). Here, Equifax's reference to the privacy policy in its Terms of Use—including specifically making "materials" sent to Equifax by consumers "subject to" the privacy policy—incorporates the policy into those terms and thus contractually obligates Equifax to protect Contract Plaintiffs' sensitive information in the manner described in the policy.

Third, Equifax contends Plaintiffs' claims are governed by a more recent privacy policy dated April 24, 2017, which stated that Equifax did not "ensure or

warrant the security of any information you transmit to us." Mot. 47. But this policy applies only to Equifax Consumer Services, LLC's "products"—and then only those purchased *on or after* April 24, 2017, meaning it does not apply to customers who purchased products before that date or who did not purchase a product but rather obtained credit reports, disputed credit items, requested a fraud alert, or froze their credit. Such actions, which constitute the bulk of the interaction between Equifax and consumers, are instead subject to Equifax's Personal Credit Reports Privacy Policy, *available at* https://www.equifax.com/privacy/personal-credit-reports/ (last updated April 18, 2013) ("Credit Reports Policy"). Mot. 47.

The Credit Reports Policy does not contain the restriction in the privacy policy relied on by Equifax. To the contrary, the Credit Reports Policy affirmatively represents that Equifax is committed to securing consumer information, limits access to certain employees, and uses "reasonable physical, technical and procedural safeguards" to ensure its protection. Compl. ¶¶ 402-04. Such language imposes contractual obligations. *See, e.g.*, *In re JetBlue*, 379 F. Supp. 2d at 324-25 (describing the substance of JetBlue's privacy policy as a "promise by JetBlue not to disclose passengers' personal information to third parties" and rejecting *In re Nw. Airlines Privacy Litig.*, 2004 WL 1278459, at *5-6 (D. Minn. June 6, 2004) as relying on an "overly narrow" reading of the

pleadings); *In re Google, Inc. Privacy Policy Litig.*, 58 F. Supp. 3d 968, 986-87 (N.D. Cal. 2014) (plaintiffs stated a claim for breach of Android phone application privacy policies, when those policies stated Google "restrict[s] access to personal information to Google employees . . . who need to know that information" and that those individuals were bound by confidentiality obligations).

B. The Complaint Sufficiently Alleges An Implied Contract Claim.

The Contract Plaintiffs also plead an alternative claim for breach of an implied contract. This Court should reject Equifax's argument that the existence of an express contract requires dismissal of the implied contract claim because "courts routinely allow plaintiffs to plead both express contract and implied contract theories, as long as those theories are clearly pled in the alternative," as they are here. *Yahoo!*, 2017 WL 3727318, at *47 (largely denying motion to dismiss implied breach of contract claim based on terms of service and privacy policy). Moreover, as shown above, the express contract on which Equifax relies—the Equifax Product Agreement—does not apply to this case by its own terms.

Similarly, the Court should reject Equifax's argument that Plaintiffs have not sufficiently identified the subject matter of and the promises contained in the implied contract. Plaintiffs allege the contract arose when they provided "Personal Information to Equifax subject to its Privacy Policy," and the policy promised to

protect the Plaintiffs' information. Compl. ¶¶ 410-11. Such allegations, in fact, are sufficient. *See, e.g.*, *Walters v. Kimpton Hotel & Rest. Grp., LLC*, 2017 WL 1398660, at *2 (N.D. Cal. Apr. 13, 2017) ("Walters plausibly alleged the existence of an implied contract arising from Kimpton's privacy policy, which states that Kimpton is 'committed' to safeguarding customer privacy and personal information. To the extent this commitment creates an enforceable promise, the promise is a voluntary duty not imposed by law and constitutes valid consideration."); *Enslin v. The Coca-Cola Co.*, 136 F. Supp. 3d 654, 675 (E.D. Pa. 2015), *aff'd sub nom.*, 2018 WL 3060098 (3d Cir. June 20, 2018) (denying motion to dismiss implied contract claim in data breach case when criminals stole laptops containing personal information of 74,000 Coca-Cola employees).

Finally, Equifax tries to impose a heightened pleading standard, demanding that Plaintiffs plead the "who, what, when, where, and why" of the claim. Mot. 49. But Rule 8 does not demand such detail. Equifax promised to protect Plaintiffs' information and Plaintiffs submitted their information to Equifax after those promises were made. No more is needed for an implied contract claim.

III. PLAINTIFFS STATE FEDERAL CLAIMS UNDER THE FAIR CREDIT REPORTING ACT.

A. Plaintiffs And The Nationwide Class Plausibly Allege A Claim Under FCRA Sections 1681b & 1681e.

The purpose of FCRA is to protect the privacy of consumer data and limit the circumstances under which it can be disseminated by a CRA such as Equifax. *See Tonge v. Fundamental Labor Strategies, Inc.*, 277 F. Supp. 3d 809, 812 (E.D. Pa. 2017). Plaintiffs allege Equifax violated FCRA by disseminating their confidential data in ways not permitted by the Act and thus Equifax is liable for damages under 15 U.S.C. §§ 1681o & 1681n(a). In response, Equifax argues that the technical requirements of a FCRA claim are not met because it did not "furnish" information to the hackers and the stolen data is not a "consumer report." Plaintiffs acknowledge that there is case law support for Equifax's position, but the decisions on which Equifax relies are neither binding here nor persuasive under the unique facts of this case.

The FCRA itself does not define the term "furnish" and thus does not directly answer the question of whether Equifax's actions are sufficient to meet that requirement. Several courts have held that the "term requires an affirmative act on the part of the consumer reporting agency," *Galaria v. Nationwide Mut. Ins. Co.*, 2017 WL 4987663, at *4 (S.D. Ohio Aug. 16, 2017), and that allowing

information to be stolen is not enough because "[t]heft victims don't 'provide' a thief with stolen goods." *See id.* (quoting *In re Experian Data Breach Litig.*, 2016 WL 7973595, at *2 (C.D. Cal. Dec. 29, 2016)). Assuming arguendo that an affirmative act is required, Plaintiffs assert Equifax committed such acts by intentionally shortchanging their data security measures and so wantonly disregarding the risk that for all practical purposes it knowingly exposed Plaintiffs' data to hackers. Compl. ¶ 325. *See, e.g.*, *Chrysler Group, LLC v. Walden*, 339 Ga. App. 733, 737 (2016) (wanton conduct is that which "is so reckless or so charged with indifference to the consequences as to be the equivalent in spirit to actual intent.") (internal citation omitted).

Equifax's conduct is analogous to an owner who leaves an expensive car in a high crime area with the windows down, the doors unlocked, and the key in the ignition and then files an insurance claim after the inevitable theft. While the owner may not have turned the key, surely a jury could find that the owner was not an innocent victim, but rather was an active participant in the crime. Here, Plaintiffs allege that, like the car owner, Equifax's conduct was so egregious and the risks were so immense that Equifax was effectively an active participant in the data breach and thus "furnished" Plaintiffs' data to the hackers within the meaning of the FCRA. Whether the evidence will ultimately support Plaintiffs' allegations

cannot be determined at this stage of the litigation. *Cf. Manuel v. Wells Fargo Bank, N.A.*, 123 F. Supp. 3d 810, 822-23 (E.D. Va. 2015) (denying summary judgment; whether CRA took an "adverse action" under FCRA is a question of fact for the jury). But certainly allegations Equifax did nothing despite explicit and repeated warnings by outside experts that its security measures were so bad the chances of an imminent data breach were 50 percent are sufficient to cross the threshold of plausibility.

The *Galaria* and *Experian* decisions relied on by Equifax are distinguishable based on the extent of the defendants' wrongdoing and the nature of their conduct. Each of the defendants in those cases was much closer to a mere "theft victim" who fell prey to sophisticated hackers, unlike Equifax which Plaintiffs allege was effectively complicit in the breach. As Congressman Walden put it: "It is like the guards at Fort Knox forgot to lock the doors and failed to notice the thieves were emptying the vaults." *Oversight of the Equifax Data Breach: Answers for Consumers*, Subcommittee on Digital Commerce and Consumer Protection (Oct. 3, 2017), at 11. In fact, the situation is even worse than the Congressman imagined. Using his analogy, it is like the guards knew the thieves were outside and planning to come in, but intentionally decided not to lock the door because it was too much trouble, and looked the other way while the vaults were emptied. On these facts,

the issue of whether Equifax "furnished" Plaintiffs' information to the hackers cannot be addressed under Rule 12.

Equifax next argues that the very reason it kept information on the 150 million Americans involved in the breach—to determine their credit worthiness—should be ignored, because the information taken by hackers is not a "consumer report." Mot. 13-14. But FCRA defines "consumer report" broadly to include consumers' credit worthiness, credit standing, credit capacity, character, general reputation, personal characteristics, or mode of living. 15 U.S.C. § 1681a(d)(1). This definition is not "very demanding" because "almost any information about consumers arguably bears on their personal characteristics or mode of living." *Trans Union Corp. v. F.T.C.*, 245 F.3d 809, 813 (D.C. Cir. 2001); *see Hoke v. Retail Credit Corp.*, 521 F.2d 1079, 1081 (4th Cir. 1975) (A consumer report "is virtually any information communicated by a consumer reporting agency" for any one of the purposes enumerated.). Contrary to Equifax's claim, characterizing the information as "header data" is not determinative. *See Parker v. Equifax Info. Servs., LLC*, 2017 WL 4003437, at *3 (E.D. Mich. Sept. 12, 2017) ("depending on context, header data may well function effectively as a consumer report.").

The stolen information certainly bears on Plaintiffs' "personal characteristics" and "mode of living." Compl. ¶¶ 318-319; 15 U.S.C. §

1681a(d)(1). It includes names, dates of birth, Social Security numbers, addresses, gender identifiers, phone numbers, driver's license numbers and states of issuance, addresses, payment card information, and Tax IDs, Compl. ¶¶ 212-213, which is the type of information courts have determined constitutes a consumer report. *See Ernst v. Dish Network, LLC*, 49 F. Supp. 3d 377, 382 (S.D.N.Y. 2014) (driver's license information bears on "mode of living"); *Klonsky v. RLI Ins. Co.*, 2012 WL 1144031, at *3 (D. Vt. April 4, 2012) (personal information beyond basic identifying data conveys information about personal characteristics and mode of living).

The motion to dismiss the FCRA claims should be denied because, under the circumstances, Plaintiffs plausibly allege that Equifax furnished consumer report information in the breach.

B. The FCRA Disclosure Subclass States A Claim For Inadequate Disclosures Under Section 1681g.

FCRA Section 1681g(a)(1) gives consumers the right to seek "[a]ll information" contained in their consumer files maintained by the credit reporting agencies. 15 U.S.C. § 1681g(a)(1). This Court has held that a request for a report under section 1681g entitles consumers to their "complete file"—not simply the information included on a consumer report prepared for the benefit of third parties. *See Taylor v. Screening Reports, Inc.*, 294 F.R.D. 680, 684-85 (N.D. Ga. 2013)

(holding that a consumer's general request for his "report" triggered an obligation to disclose all information in consumer's file under section 1681g). Section 1681g(a)(3) requires CRAs to identify "each person" that procured a consumer report for any purpose other than employment during the 1-year period preceding the date on which the request is made. 15 U.S.C. § 1681g(a)(3)(ii). These disclosures must be made "clearly and accurately." 15 U.S.C. § 1681g(a).

After Equifax discovered the breach on July 29, 2017, it made section 1681g disclosures to consumers who requested their files. The FCRA Disclosure Subclass comprised of such consumers asserts that Equifax's disclosures did not inform them a breach had occurred and their information had been furnished to unauthorized people, violating FCRA. Compl. ¶¶ 21, 105, 419. Equifax argues that Plaintiffs' claim fails because the hackers did not access a "consumer report." But for the same reasons explained above, the information disclosed in the breach satisfies the broad definition of "consumer report" under the statute.

Equifax also argues that a data breach does not trigger FCRA's disclosure obligations because "a CRA generally has no way of knowing" the identities of the "criminal hackers who infiltrated its systems." Mot. 67. But this, of course, is a factual question, and the parties cannot assume prior to discovery that the identities of the hackers were unknowable. *See F.T.C. v. Citigroup, Inc*., 239 F. Supp. 2d

1302, 1305 (N.D. Ga. 2001) ("A motion to dismiss concerns only the complaint's legal sufficiency and is not a procedure for resolving factual questions or for addressing the merits of the case."). Moreover, even if Equifax was unable to identify the hacker's precise identity, the purpose of the disclosure requirement under section 1681g(a)(3) is to keep consumers informed about who has accessed their information. By failing to include even a general description of the breach and those responsible for it, Equifax deprived consumers of their right to receive "clear and accurate" disclosures in violation of section 1681g(a) and the opportunity to take measures to mitigate possible identity theft and fraud.

For this reason, Equifax's conclusory statement that section 1681g(a)(3) "clearly contemplates" a third party obtaining a consumer report "in the ordinary course of business" and that it would be "absurd" to apply the disclosure requirement in this context carries little weight. Mot. 66-67. Congress enacted FCRA "out of concerns about abuses in the consumer reporting industry," *Dalton v. Capital Assoc. Indus, Inc.*, 257 F.3d 409, 414 (4th Cir. 2001), and "to protect consumer privacy." *TRW Inc. v. Andrews*, 534 U.S. 19, 23 (2001) (citing 15 U.S.C. § 1681(a)). "These consumer oriented objectives support a liberal construction of the FCRA." *Cortez v. Trans Union, LLC*, 617 F.3d 688, 706 (3d Cir. 2010). Permitting Plaintiffs to seek redress under section 1681g for Equifax's decision not

to disclose the breach when consumers inquired about their files thus is not absurd, but furthers the underlying statutory purpose.

IV. PLAINTIFFS PLEAD VIABLE STATE STATUTORY CLAIMS.

A. Plaintiffs State Viable Consumer Protection Claims.

1. Equifax's Request To Dismiss Consumer Protection Claims On Grounds Of Extraterritoriality Should Be Rejected.

Equifax seeks dismissal of various state consumer protection statutes on the ground that they cannot govern conduct that took place in Georgia. This argument fails because even though Equifax's misconduct may have emanated from Georgia, it injured consumers nationwide. Equifax cites authority from eight states, claiming their consumer statutes do not protect against wrongful conduct in Georgia. But that case law shows that—irrespective of where the wrongful conduct emanated—if the misconduct injures people within the state that enacted the statute, the statute protects that state's consumers.[13]

---

[13] *E.g.*, *McKinnon v. Dollar Thrifty*, 2013 WL 791457, at *5 (N.D. Cal. Mar. 4, 2013) (California); *Rogers v. Omni Sol.*, 2010 WL 4136145, at *4 n.2 (S.D. Fla. Oct. 19, 2010) (Florida); *Van Tassell v. United Mktg. Grp.*, 795 F. Supp. 2d 770, 781-82 (N.D. Ill. 2011) (Illinois); *State ex rel. Nixon v. Estes*, 108 S.W.3d 795, 800 (Mo. Ct. App. 2003) (Missouri); *Cruz v. FXDirectDealer*, 720 F.3d 115, 122 (2d Cir. 2013) (New York); *ITCO v. Michelin Tire*, 722 F.2d 42, 49 (4th Cir. 1983) (North Carolina); *Browne v. World Christian Church*, 2001 WL 681256, at *3 (W.D. Tex. Apr. 5, 2001) (Texas); *Martin v. LG Elecs.*, 2015 WL 1486517, at *3 (W.D. Wis. Mar. 31, 2015) (Wisconsin).

The same point holds for Equifax's citation to cases like *State Farm v. Campbell*, 538 U.S. 408 (2003). None of those cases prohibits states from protecting their consumers against out-of-state tortfeasors who cause injury to those consumers. *See, e.g.*, *Crouch v. Teledyne Cont'l Motors*, 2011 WL 1539854, at *3-4 (S.D. Ala. Apr. 21, 2011) (*State Farm* does not apply where the "alleged out-of-state conduct resulted in injury to the Plaintiffs" in their home states); *Boyd v. Goffoli*, 216 W. Va. 552, 561-63 (2004) (same); *Jacobson v. R.J. Reynolds Tobacco*, 2013 WL 12094893, at *4 (S.D. Fla. Sept. 12, 2013) (same).

Equifax implicitly acknowledges that its argument hinges on there being no "harmful effect" outside of Georgia. Mot. 55. But unbelievably—given that Equifax does business across the country, its misrepresentations and omissions extended nationwide, and nearly 150 million Americans were impacted by the breach—Equifax does not admit such harm occurred. Equifax concedes only that "*if* any harmful effect was felt in any other state," it is not responsible because the harm allegedly was proximately caused by the hackers—not Equifax. *Id.* (emphasis added). As discussed above, however, Equifax cannot escape responsibility if the hackers' actions were foreseeable. Whether harm occurred outside of Georgia and whether Equifax should have foreseen that harm are fact

issues that cannot be resolved now. Equifax's challenge to the application of consumer protection statutes of states other than Georgia thus should be rejected.

2. Plaintiffs Have Adequately Pleaded Fraud Where Necessary.

Plaintiffs have pleaded those claims that sound in fraud with sufficient specificity under Rule 9(b). Equifax's argument to the contrary is wrong. Mot. 56.

Claims are subject to Rule 9(b) only if they "require allegations of [common law] fraud" or "sound in fraud." *In re AFC Enters., Inc. Sec. Litig.*, 348 F. Supp. 2d 1363, 1376 (N.D. Ga. 2004). In contrast, claims are not subject to Rule 9(b) merely because they are "fraud-like." *F.T.C. v. Hornbeam Special Situations, LLC*, 2018 WL 1870094, at *3 (N.D. Ga. Apr. 16, 2018). Most UDAP statutes do not require proof of common law fraud. *See* Appendix A hereto. As a result, claims under these statutes are only subject to Rule 9(b) if they "sound in fraud."

A claim "sounds in fraud" where the plaintiff alleges "a unified course of fraudulent conduct and relies entirely on that course of conduct as the basis of that claim." *Burgess v. Religious Tech. Ctr., Inc.*, 2014 WL 11281382, at *6 (N.D. Ga. Feb. 19, 2014), *aff'd*, 600 F. App'x 657 (11th Cir. 2015). Here, the UDAP deception claims do not rely entirely on a single course of fraudulent conduct. *See id.* A core allegation focuses on Equifax's failure to stop or prevent the data breach, not just its failure to disclose the truth about its poor data security. *E.g.*,

Compl. ¶ 216 (noting that "little priority was given to even rudimentary data security protocols," according to the Warren Report).

The facts in this case are starkly different than in the cases Equifax cites, which involve narrow representations to individuals rather than broad representations that affect all Americans pursuant to a statutory scheme that allows Equifax to amass its massive troves of data. *See* Mot. 56-57 (citing *Crespo v. Coldwell Banker Mortg.*, 599 F. App'x 868, 873 (11th Cir. 2014) (pro se plaintiffs alleged they were "duped" into contracting with a mortgage originator because he later sold the mortgage to another company); *Am. Dental Ass'n v. Cigna Corp.*, 605 F.3d 1283, 1291 (11th Cir. 2010) (three dentists alleged dental association promised higher reimbursement rates than they actually received)).[14]

3. No Claims Should Be Dismissed For Failure To Allege Scienter.

Equifax seeks dismissal of 49 state law claims based on the purported failure "to sufficiently plead scienter." But Equifax cites zero authority that scienter is an element of those claims, justifying denial of its motion on that basis alone. In any event, the Complaint devotes dozens of paragraphs to Equifax's knowledge and intent. *See, e.g.*, Compl. ¶¶ 1, 146-47, 150, 156-65 (Equifax understood the cybersecurity threats and knew it was obligated safeguard personal information);

[14] Plaintiffs address Equifax's reliance argument in Section I.C above.

¶¶ 147-49, 151-55 (Equifax claimed it was capable of safeguarding personal information and never let on that its cybersecurity measures were lacking); ¶¶ 158, 166-95, 216-26 (Equifax consciously deprioritized cybersecurity and opted for a slate of inadequate measures, despite explicit warnings). In the face of these allegations, whether Equifax had the requisite level of any required scienter cannot be resolved at the pleading stage.

4. Plaintiffs Sufficiently Allege Injury.

Equifax cursorily argues that Plaintiffs have not alleged adequate injuries under consumer statutes that require "ascertainable and monetary" injuries. Mot. 60-61. This argument should be rejected. Equifax cites one California case for the proposition that Plaintiffs were not injured by an increased risk of identity theft, forcing them to spend time and money on credit monitoring and other prophylactic measures, and diminishing the value of their personal information. But that case is inapplicable to any of the non-California claims, and other California district courts have found such allegations sufficient. *See Corona v. Sony Pictures Entm't, Inc.*, 2015 WL 3916744, *5 (C.D. Cal. June 15, 2015); *Witriol v. LexisNexis Grp.*, 2006 WL 4725713, *6 (N.D. Cal. Feb. 10, 2006). The California Supreme Court is in accord. *Kwikset Corp. v. Superior Court*, 51 Cal. 4th 310, 323 (2011).

5. Plaintiffs' Claims Involve Consumer Transactions.

Both non-Contract and Contract Plaintiffs have alleged transactions connected to Equifax's unfair and deceptive practices and all Plaintiffs allege that they participate in a consumer credit system in which Equifax plays an integral part, acquiring information on virtually all of their commercial activity. Equifax nonetheless asks the Court to dismiss the claims of Plaintiffs from twenty-five states, arguing they did not participate in a "commercial transaction *with Equifax*." Mot. 61 (emphasis added). But Equifax provides no case law for 18 of those states and only cites one case in its brief. *See* Mot. 61-62 & Ex. 2. This is likely because courts routinely hold that technical privity between the parties is unnecessary to pursue claims under the statutes at issue. *See* Appendix B.[15] Courts thus have permitted claims by plaintiffs against wholesalers, debt collectors, mortgage servicers, third-party conspirators, business competitors, and other third-parties to consumer transactions. *Id*.

6. Equifax Owed A Duty Of Disclosure Under State Consumer Statutes.

Equifax argues it is not liable under 17 states' consumer protection statutes because it had no duty to disclose its grossly inadequate cybersecurity measures. Yet, under all 17 states' laws, a duty to disclose arises when a defendant has

[15] Plaintiffs abandon Count 31 under the Idaho Consumer Protection Act.

voluntarily spoken but failed to disclose the whole truth, the defendant has exclusive knowledge of information that would be material to consumers, the statute itself imposes a duty to disclose, or where other relevant factors are met. *See* Appendix C.

The Complaint avers Equifax repeatedly made statements that required correction, boasting about its data security bona fides and telling consumers that "You'll feel safe with Equifax"; Equifax "built [its] reputation on [its] commitment to . . . protect the privacy and confidentiality of personal information about consumers"; and Equifax had "security protocols and measures in place to protect . . . personally identifiable information." *See* Compl. ¶¶ 1, 146-55, 166-75, 194, 216, 220-21, 224. Moreover, Equifax had exclusive knowledge of the deficiency of its data security. There was no way a reasonable consumer could have learned about Equifax's security controls without Equifax disclosing the information. These allegations satisfy the multi-factor tests of the applicable states. *See* Appendix C. Finally, Plaintiffs' claims in Hawaii, Maryland, New Mexico, and Texas include enumerated statutory violations that impose a statutory duty to disclose. *Id.* Thus, Equifax owed a duty to disclose under each of those statutes.

7. Equifax Mischaracterizes Plaintiffs' Equitable Claims.

Equifax incorrectly argues that Plaintiffs seek money damages under four claims that permit only injunctive relief. *See* Mot. 63. None of Equifax's arguments support dismissal. Money damages are available for a violation of the Illinois Personal Information Protection Act, 815 ILCS § 530/10. Such a violation constitutes an unlawful practice under the Illinois Consumer Fraud and Deceptive Business Practices Act, 815 ILCS § 505 *et seq.*, which expressly permits suits for damages. *See* 815 ILCS § 505/10a(a); *see also Barnes & Noble*, 887 F.3d at 829 (reversing dismissal of data breach plaintiffs' claims under this statute).

Equifax also misconstrues Plaintiffs' claims under the Maine, Minnesota, and Nebraska Uniform Trade Secrets Acts. Plaintiffs do not seek money damages under these statutes, but merely request "all monetary and non-monetary relief allowed by law." *See* Compl. ¶¶ 805 (Maine), 890 (Minnesota), and 954 (Nebraska). Monetary relief in the form of attorneys' fees and costs is available under each statute. *See* 10 M.R.S.A. § 1213 (Maine); M.S.A. § 325D.45 (Minnesota); N.R.S.A. § 87-303 (Nebraska). While the Maine claim inadvertently mentions "damages or restitution," that clause is rendered inoperative by the "allowed by law" limitation earlier in the sentence. *See* Compl. ¶ 805. Accordingly, the Court should deny Equifax's motion to dismiss these claims.

8. Plaintiffs' Massachusetts And Nevada Claims Are Privately Enforceable.

Equifax provides no basis for dismissing Plaintiffs' claims under either the Massachusetts Consumer Protection Act ("MCPA") or the Nevada Deceptive Trade Practices Act ("NDTPA"). *See* Mot. 64. Contrary to Equifax's position, the MCPA is privately enforceable, including in data breach cases. *See, e.g.*, *In re TJX*, 564 F.3d at 498 (affirming denial of motion to dismiss MCPA claims brought by consumer data breach victims).[16] Similarly, Equifax erroneously claims that the NDTPA may be enforced only by district attorneys and the elderly. *See* Mot. 64 (citing N.R.S. §§ 598.0983-0989). Chapter 41 of the Nevada Code provides a private right of action under this and many other statutes. *See* N.R.S. § 41.600(1)-

[16] Equifax cites one federal ruling dismissing a plaintiff's MCPA claim, which reasoned that a violation of the Massachusetts Security Breach statute does not constitute an MCPA violation. Mot. 64 (citing *Katz v. Pershing, LLC*, 806 F. Supp. 2d 452 (D. Mass. 2011)). But the security breach statute is just one of several independent bases for Plaintiffs' claim, *see* Compl. ¶ 846(a)-(g), and Equifax does not challenge the sufficiency of the relevant allegations. Regardless, *Katz* is of limited, if any, help to Equifax. On appeal, the First Circuit refused to adopt the district court's reasoning. *Katz v. Pershing, LLC*, 672 F.3d 64, 78 (1st Cir. 2012) (affirming dismissal on other grounds). And, since *Katz* was decided, Massachusetts courts have continued to hold that MCPA claims based on violations of statutes enacted to protect the public are viable. *See Klairmont v. Gainsboro Rest., Inc.*, 465 Mass. 165, 172 (2013) (MCPA claim based on building code violations that private parties cannot otherwise enforce); *see also Adams v. Cong. Auto Ins. Agency, Inc.*, 90 Mass. App. 761, 771-72 (2016), *review denied*, 477 Mass. 1101 (2017) (implicitly recognizing a private MCPA claim predicated on Mass. Gen. Law 93H, but dismissing it as insufficiently pled).

(2)(e) ("An action may be brought by any person who is a victim of . . . a deceptive trade practice as defined in NRS 598.0915 to 598.0925").

B. Plaintiffs Properly State Claims Under State Data Breach Statutes.

1. Data Breach Notification Statutes.

States have enacted laws requiring companies such as Equifax to notify consumers when they learn that their data security systems have been breached.[17] Thirty state statutes allow a private right of action. But Equifax asserts that in twelve of those states citizens cannot assert a statutory claim. With regard to Iowa, Michigan, and New York, this argument ignores the statutory language, *see* Iowa Code § 715.C.2(9)(b); Mich. Comp. Laws § 445.72(15); N.Y. Gen. Bus. Law § 899-aa (6)(b); and how that language has been interpreted in other data breach actions. *Target*, 66 F. Supp. 3d at 1169 (finding Iowa and Michigan notification statutes' savings clauses sufficient to provide private right of action). While a trial court found that the New York statute does not confer a private right of action, this Court is only bound state appellate court decisions, *see Bravo v. United States*, 577 F.3d 1324, 1326 (11th Cir. 2009), and the trial court ruling is unpersuasive for the

[17] *See Security Breach Notification Laws*, NAT'L. CONF. OF STATE LEGISLATURES (Mar. 29, 2018), http://www.ncsl.org/research/telecommunications-and-information-technology/security-breach-notification-laws.aspx.

same reasons *Target* allowed consumers' claims to proceed under the Michigan and Iowa statutes.

In four other states where Equifax argues there is no private right of action—Connecticut, Maryland, Montana and New Jersey—violations of the notification statutes are unfair trade practices and thus can be privately enforced through those states' consumer protection statutes. *See* C.G.S.A. § 36a-701b(g) (violations are unfair trade practices enforceable through C.G.S.A. § 42-110b); Md. Comm. Code § 14-3508 (violations are unfair trade practices enforceable through Md. Comm. Code § 13-408(a)); Mont. Code Ann. § 30-14-1705 (violations of notification law are violations of Mont. Code Ann. § 30-14-103 and enforceable through Mont. Code Ann. § 30-14-133(1)); N.J. Stat. Ann. § 56:8-166 (violations of N.J. Stat. Ann. § 56:8-163 are violations of N.J. Stat. Ann. §§ 56:8-1, *et seq.*, and enforceable through N.J. Stat. Ann. § 56:8-19).[18]

[18] Equifax relies heavily for its argument on *Torres v. Wendy's International, LLC*, 2017 WL 8780453, at *6 (M.D. Fla. March 21, 2017). That case relied on *Holmes v. Countrywide Fin. Corp.*, 2012 WL 2873892, at *13 (W.D. Ky. July 12, 2012) to hold that New Jersey's statute does not provide a private right of action. The Court in *Holmes* relied on N.J. Stat. Ann. § 56:8-163 without addressing N.J. Stat. Ann. § 56:8-166's declaration that violations of § 56:8-163 violate the New Jersey Consumer Fraud Act, N.J. Stat. Ann. §§ 56:8-1, *et seq*. Violations of the New Jersey Consumer Fraud Act are enforceable by consumers through § 56:8-19. *See Dugan v. TGI Fridays, Inc.*, 231 N.J. 24, 52 (2017).

Four more states that Equifax claims do not provide a private right of action—Colorado, Delaware, Kansas, and Wyoming—have statutory language stating that the "provisions of this section are not exclusive." *Target*, 66 F. Supp. 3d at 1169. *Target* permitted these claims to proceed because the statutes' "permissive" language supported private enforcement. *Id*. As in *Target*, Equifax's arguments for dismissal of these claims fail.

The last two notification statutes that Equifax claims lack a private enforcement mechanism—Georgia and Wisconsin—are silent on the issue. *See* O.C.G.A. § 10-1-912; Wis. Stat. § 134.98. In *Target*, claims under both statutes were permitted to proceed because there was no authority suggesting that silence should be interpreted to prohibit such claims. *Id.* at 1169-70. Equifax cites no authority on point to contradict the *Target* court's decision, but instead relies on an unrelated Georgia case finding no right of action in a statute that gives the Georgia Insurance Commissioner exclusive enforcement authority over particular automobile policy issues. *State Farm Mut. Auto. Ins. Co. v. Hernandez Auto Painting and Body Works, Inc.*, 312 Ga. App. 756, 761 (2011). Because nothing in that case addresses the precise question presented here, this Court should follow the *Target* analysis and allow the claim to proceed.

Equifax's next argues for dismissal of claims under the notification statutes because Plaintiffs' allegedly made "concessions" regarding Equifax's reaction to the breach. These "concessions" are merely Equifax's mischaracterizations of Plaintiffs' factual allegations for the purpose of enabling the argument that it provided prompt notice of the breach and thus did not violate any notification statute. The Court, of course, must decide the motion based on Plaintiffs' allegations, not the spin Equifax puts on them, *Home Depot*, 2016 WL 2897520, at *3. Plaintiffs have plausibly pled the basis for a violation.

Equifax also mischaracterizes the time required for notification under eight statutes to argue it provided timely notice as a matter of law. That argument is not supported by the eight statutes on which it relies. Two of the statutes mandate notice in the "most expedient time possible and without unreasonable delay," Cal. Civ. Code § 1798.82(a); N.Y. Gen. Bus. Law § 899-aa(2), and five require notice within a reasonable time, but in no event later than a specified number of days. *See* C.G.S.A. § 36a-701b(b)(1); 6 Del. Code Ann. § 12B-102(c); Md. Comm. Code § 14-3504(c)(2); Wash. Rev. Code § 19.255.010(16); Wis. Stat. § 134.98(3).[19]

[19] Only one statute, Tenn. Code Ann. § 47-18-2107(b), does not expressly require notice within a reasonable time, mandating notice no later than 45 days "from the discovery or notification of the breach of system security." But the precise date

Finally, Equifax argues that "no Plaintiff has pleaded facts sufficient to show that he or she suffered injury as a result of any delay in notification" and thus Plaintiffs' claims under the notification statutes must be dismissed. Mot. 68. However, as discussed above, Plaintiffs have alleged legal cognizable injuries and have specifically alleged injury from the late notice, such as the lack of knowledge that it was necessary to freeze their credit or take other precautions. At this stage of the litigation, Plaintiffs have no obligation to do more. *See Target*, 66 F. Supp. 3d at 1171 ("Although Target would like a more detailed explanation of what damages were caused by the delayed breach notification, the allegations in the Complaint are not fatally insufficient [and] plausibly allege[] that Plaintiffs suffered damage as a result of the delay."). Equifax's argument is nothing more than a premature attack on causation, which must await summary judgment or trial.

2. Maryland Social Security Number Privacy Act.

Equifax argues that Plaintiffs do not have a private right of action under the Maryland Social Security Number Privacy Act, Md. Comm. Code §§ 14-3401, *et seq.*, relying on *Carmax Auto Superstores, Inc. v. Sibley*, 194 F. Supp. 3d 392, 402 (D. Md. 2016). The plaintiff in *Sibley*, however, did not bring an action directly under the Act, as Plaintiffs do here, but asserted a negligence per se claim. To

---

Equifax was on notice of the breach, whether Equifax recognized it or not, is a fact issue that cannot be resolved on a Rule 12(b)(6) motion.

determine whether a statute allows a private right of action, Maryland courts use a three-factor test that differs from the one used to determine the validity of a negligence claim evidenced by a statutory violation. *Compare Sibley*, 194 F. Supp. 3d at 402 (D. Md. 2016) *with Fangman v. Genuine Title, LLC*, 447 Md. 683, 695 (2016). Under that test, a court must ask:

> (1) Is the plaintiff one of the class for whose special benefit the statute was enacted? (2) Is there any indication of legislative intent, explicit or implicit, either to create such a remedy or to deny one? (3) Is it consistent with the underlying purpose of the legislative scheme to imply such a remedy for the plaintiff?

Fangman, 447 Md. at 695. Each of these factors supports the existence of implied right of action. The very purpose of the Act is to protect Social Security numbers from unauthorized disclosure by companies such as Equifax. Allowing consumers a right of action when such disclosure occurs is consistent with that underlying purpose and is implicit in the structure of the Act. Surely the legislature did not intend to create a right without a remedy.

Equifax also argues that it did not "initiate" the transmission of Social Security numbers and thus did not violate the Act. This argument fails for the same reason as Equifax's argument that it did not "furnish" a credit report under FCRA, namely that Plaintiffs' allege its conduct was so egregious that for all practical

purposes Equifax was an active participant in the breach and the truth of this allegation cannot be decided on a motion to dismiss.

C. The Complaint Properly States Claims Under Puerto Rico and Virgin Islands Law.

Equifax's argument that the Complaint must identify a plaintiff from each jurisdiction is premature. It is sufficient now to allege that individuals nationwide suffered injury. *See* Compl. ¶¶ 1-6; 294-300; 1143, 1279, 1295, 1309. Addressing this same argument in *Target*, the court held that any such analysis "is best left to after the class-certification stage." 66 F. Supp. 3d at 1160; *see also, e.g.*, *Langan v. Johnson & Johnson Consumer Cos.*, 2018 WL 3542624, at *3-6 (2d Cir. July 24, 2018). Equifax's only authority is a decision addressing the issue at certification, not on a motion to dismiss. *See Griffin v. Dugger*, 823 F.2d 1476, 1482 (11th Cir. 1987). "To force Plaintiffs' attorneys to search out those individuals at this stage serves no useful purpose." *Target*, 66 F. Supp. 3d at 1160.

D. Plaintiffs Sufficiently Invoke O.C.G.A. § 13-6-11.

Under O.C.G.A. § 13-6-11, a plaintiff is entitled to recover fees and expenses as part of damages if the defendant has acted in bad faith, been stubbornly litigious, or caused unnecessary trouble or expense. This standard is met where the defendant through egregious misconduct has created a foreseeable risk of injury to others. *See, e.g.*, *Lewis v. D. Hays Trucking, Inc.*, 701 F. Supp. 2d

1300, 1312-13 (N.D. Ga. 2010) (driving a truck after driver was told he failed a DOT physical); *Ford Motor Co. v. Stubblefield*, 171 Ga. App. 331, 342 (1984) (selling an automobile despite knowledge it was defective). It is not necessary that the defendant's conduct rise to the level of an intentional tort. *Windermere, Ltd. v. Bettes*, 211 Ga. App. 177, 179 (1993). Plaintiffs plausibly allege that Equifax's conduct leading up to the breach was egregious and that both the breach and injury that resulted were foreseeable, precluding resolution at this stage of whether Plaintiffs are entitled to recovery under O.C.G.A. § 13-6-11.

CONCLUSION

For the reasons stated herein, and based on the detailed allegations in the Complaint, the Court should deny Equifax's motion to dismiss. Alternatively, if the Court determines the allegations are deficient in any way, Plaintiffs request an opportunity to amend the Complaint to address those deficiencies.

Dated: August 13, 2018

Respectfully submitted,

/s/ Amy E. Keller
Amy E. Keller
Adam J. Levitt
DICELLO LEVITT & CASEY LLC
Ten North Dearborn Street
Eleventh Floor
Chicago, Illinois 60602
Tel. 312.214.7900
akeller@dlcfirm.com
alevitt@dlcfirm.com

/s/ Norman E. Siegel
Norman E. Siegel
Barrett J. Vahle
J. Austin Moore
STUEVE SIEGEL HANSON LLP
460 Nichols Road, Suite 200
Kansas City, Missouri 64112
Tel. 816.714.7100
siegel@stuevesiegel.com
vahle@stuevesiegel.com
moore@stuevesiegel.com

Consumer Plaintiffs' Co-Lead Counsel

/s/ Kenneth S. Canfield
Kenneth S. Canfield
Georgia Bar No. 107744
DOFFERMYRE SHIELDS CANFIELD & KNOWLES, LLC
1355 Peachtree Street, N.E.
Suite 1900
Atlanta, Georgia 30309
Tel. 404.881.8900
kcanfield@dsckd.com

Roy E. Barnes
John R. Bevis
J. Cameron Tribble
BARNES LAW GROUP, LLC
31 Atlanta Street
Marietta, Georgia 30060
Tel. 770.227.6375
roy@barneslawgroup.com
bevis@barneslawgroup.com
ctribble@barneslawgroup.com

David J. Worley
EVANGELISTA WORLEY LLC
8100A Roswell Road Suite 100
Atlanta, Georgia 30350
Tel. 404.205.8400
david@ewlawllc.com

Consumer Plaintiffs' Co-Liaison Counsel

Rodney K. Strong
GRIFFIN & STRONG P.C.
235 Peachtree Street NE, Suite 400
Atlanta, Georgia 30303
Tel. 404.584.9777
rodney@gspclaw.com

Consumer Plaintiffs' State Court Coordinating Counsel

Andrew N. Friedman
COHEN MILSTEIN SELLERS & TOLL PLLC
1100 New York Avenue, NW
Suite 500
Washington, D.C. 20005
Tel. 202.408.4600
afriedman@cohenmilstein.com

Eric H. Gibbs
David M. Berger
GIRARD GIBBS LLP
505 14th Street
Suite 1110
Oakland, California 94612
Tel. 510.350.9700
ehg@classlawgroup.com

James Pizzirusso
HAUSFELD LLP
1700 K Street NW Suite 650
Washington, D.C. 20006
Tel. 202.540.7200
jpizzirusso@hausfeld.com

Ariana J. Tadler
MILBERG TADLER PHILLIPS GROSSMAN LLP
One Penn Plaza
19th Floor
New York, New York 10119
Tel. 212.594.5300
atadler@milberg.com

John A. Yanchunis
MORGAN & MORGAN COMPLEX LITIGATION GROUP
201 N. Franklin Street, 7th Floor
Tampa, Florida 33602
Tel. 813.223.5505
jyanchunis@forthepeople.com

William H. Murphy III
MURPHY, FALCON & MURPHY
1 South Street, 23rd Floor
Baltimore, Maryland 21224
Tel. 410.539.6500
hassan.murphy@murphyfalcon.com

Jason R. Doss
THE DOSS FIRM, LLC
36 Trammell Street, Suite 101
Marietta, Georgia 30064
Tel. 770.578.1314
jasondoss@dossfirm.com

Consumer Plaintiffs' Steering Committee

CERTIFICATE OF COMPLIANCE

I hereby certify pursuant to L.R. 7.1D that the foregoing complies with the font and point selections permitted by L.R. 5.1C. This brief was prepared on a computer using the Times New Roman font (14 point).

/s/ Norman E. Siegel

CERTIFICATE OF SERVICE

I hereby certify that a copy of the foregoing was filed with this Court via its CM/ECF service, which will send notification of such filing to all counsel of record this 13th day of August, 2018.

/s/ Norman E. Siegel